

From: Ritchey, Gail (COT)

Sent: Wednesday, February 13, 2008 10:06 AM

To: COT Constitutional CIO Security Contacts; COT Cabinet CIO Security Contacts; CTC Members; COT All

Cc: COT Exchange Administrators; COT Security Alert Contacts; COT Security Contact COT-Support; COT Security Contact Pass; COT Security Contact Self-Support; COT Technical Contacts; SecurityContacts Group

Subject: February Security Bulletins

COT Security Alert

Microsoft has just released the [Security Bulletins for February](#) which includes **six critical** bulletins and **five important** bulletins. Various vulnerabilities are addressed in the bulletins. Details of the vulnerabilities and their impact are provided in the links listed.

MS08-003 Important: Vulnerability in Active Directory Could Allow Denial of Service (946538)

<http://www.microsoft.com/technet/security/bulletin/MS08-003.mspx>

MS08-004 Important: Vulnerability in Windows TCP/IP Could Allow Denial of Service (946456)

<http://www.microsoft.com/technet/security/bulletin/MS08-004.mspx>

MS08-005 Important: Vulnerability in Internet Information Services Could Allow Elevation of Privilege (942831)

<http://www.microsoft.com/technet/security/bulletin/MS08-005.mspx>

MS08-006 Important: Vulnerability in Internet Information Services Could Allow Remote Code Execution (942830)

<http://www.microsoft.com/technet/security/bulletin/MS08-006.mspx>

MS08-007 Critical: Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution (946026)

<http://www.microsoft.com/technet/security/bulletin/MS08-007.mspx>

MS08-008 Critical: Vulnerability in OLE Automation Could Allow Remote Code Execution (947890)

<http://www.microsoft.com/technet/security/bulletin/MS08-008.mspx>

MS08-009 Critical: Vulnerability in Microsoft Word Could Allow Remote Code Execution (947077)

<http://www.microsoft.com/technet/security/bulletin/MS08-009.msp>

MS08-010 Critical: Cumulative Security Update for Internet Explorer (944533)

<http://www.microsoft.com/technet/security/bulletin/MS08-010.msp>

MS08-011 Important: Vulnerabilities in Microsoft Works File Converter Could Allow Remote Code Execution (947081)

<http://www.microsoft.com/technet/security/bulletin/MS08-011.msp>

MS08-012 Critical: Vulnerabilities in Microsoft Office Publisher Could Allow Remote Code Execution (947085)

<http://www.microsoft.com/technet/security/bulletin/MS08-012.msp>

MS08-013 Critical: Vulnerability in Microsoft Office Could Allow Remote Code Execution (947108)

<http://www.microsoft.com/technet/security/bulletin/MS08-013.msp>

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

**Commonwealth Office of Technology
Division of Technical Services
Security Administration Branch**

120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601

COTSecurityServices@ky.gov

<http://technology.ky.gov/security/>